



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/913,884	03/08/2002	Jean-Sebastien Coron	032326-161	5848

21839 7590 11/29/2005

BUCHANAN INGERSOLL PC
(INCLUDING BURNS, DOANE, SWECKER & MATHIS)
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER

HENNING, MATTHEW T

ART UNIT

PAPER NUMBER

2131

DATE MAILED: 11/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/913,884

Applicant(s)

CORON ET AL.

Examiner

Matthew T. Henning

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 17 August 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-8, 10 and 13-23 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-8, 10 and 13-23 is/are rejected.
- 7) ☒ Claim(s) 6-8 and 15-18 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 08 March 2002 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>8/17/2001</u> | 6) <input type="checkbox"/> Other: _____ |

Art Unit: 2131

1 This action is in response to the communication filed on 8/17/2001.

2 **DETAILED ACTION**

3 Claims 1-8, 10, and 13-23 have been examined.

4 ***Title***

5 The title of the invention is acceptable.

6 ***Priority***

7 This application is a 371 of PCT/FR00/00130 which claims priority to France 99/01937
8 filed 2/17/1999.

9 Therefore, the effective filing date for the subject matter defined in the pending claims in this
10 application is 2/17/1999.

11 ***Information Disclosure Statement***

12 The information disclosure statement(s) (IDS) submitted on 8/17/2001 are in compliance
13 with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information
14 disclosure statements.

15 ***Drawings***

16 The drawings are objected to because the drawings (i.e. Fig. 2) contain French text.

17 The drawings are further objected to under 37 CFR 1.83(a). The drawings must show
18 every feature of the invention specified in the claims. Therefore, the details of the random data
19 and processing of the random data must be shown or the feature(s) canceled from the claim(s).
20 No new matter should be entered.

21 Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to
22 the Office action to avoid abandonment of the application. Any amended replacement drawing

1 sheet should include all of the figures appearing on the immediate prior version of the sheet,
2 even if only one figure is being amended. The figure or figure number of an amended drawing
3 should not be labeled as “amended.” If a drawing figure is to be canceled, the appropriate figure
4 must be removed from the replacement sheet, and where necessary, the remaining figures must
5 be renumbered and appropriate changes made to the brief description of the several views of the
6 drawings for consistency. Additional replacement sheets may be necessary to show the
7 renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an
8 application must be labeled in the top margin as either “Replacement Sheet” or “New Sheet”
9 pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will
10 be notified and informed of any required corrective action in the next Office action. The
11 objection to the drawings will not be held in abeyance.

12 *Claim Objections*

13 Claims 6-8, and 15-18 are objected to because of the following informalities: Claims 6
14 and 8 contain the limitation “cryptography algorithm” instead of “cryptographic algorithm”.
15 Appropriate correction is required.

16 *Claim Rejections - 35 USC § 102*

17 The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the
18 basis for the rejections under this section made in this Office action:

19 *A person shall be entitled to a patent unless –*

20 *(e) the invention was described in (1) an application for patent, published under section*
21 *122(b), by another filed in the United States before the invention by the applicant for patent or*
22 *(2) a patent granted on an application for patent by another filed in the United States before the*
23 *invention by the applicant for patent, except that an international application filed under the*
24 *treaty defined in section 351(a) shall have the effects for purposes of this subsection of an*

1 *application filed in the United States only if the international application designated the United*
2 *States and was published under Article 21(2) of such treaty in the English language.*
3

4 Claims 1-8, 10, and 13-23 are rejected under 35 U.S.C. 102(e) as being anticipated by
5 Kocher et al. (US Patent Number 6,278,783) hereinafter referred to as Kocher.

6 Regarding claim 1, Kocher disclosed a countermeasure method in an electronic
7 component using a cryptographic algorithm with a secret key K on an input message (M), of the
8 type in which an operation (OPN) or a sequence of operations comprising a bit by bit
9 manipulation of an input data item (D) is executed, in order to supply an output data item
10 (OPN(D)) (See Kocher Abstract), said operation comprising the following steps: drawing a first
11 random data item (U), having the same size as the input data item (D) (See Kocher Col. 6 Lines
12 39-42); calculating a second random data item (V), by performing an exclusive OR operation
13 between the input data item and the first random data item (U) (See Kocher Col. 6 Lines 39-42);
14 executing the operation (OPN) or the sequence of operations on the first random data item (U)
15 and the second random data item (V), to thereby generate respectively a first random result
16 (OPN(U)) and a second random result (OPN(V)) (See Kocher Col. 6 Lines 47-49).

17 Regarding claim 19, Kocher disclosed An electronic security component of the type in
18 which a cryptographic algorithm with a secret key is applied to an input message using bit-by-bit
19 manipulation of an input data item D to calculate an output data item (See Kocher Abstract),
20 comprising: means for generating a first random data item U having the same size as said input
21 data item D (See Kocher Col. 6 Lines 39-42); means for performing an exclusive-OR operation
22 on said input data item D and said first random data item U, to generate a second random data
23 item V (See Kocher Col. 6 Lines 39-42); and means for executing said bit-by-bit manipulation

1 on said first random data item U and said second random data item V to generate a first random
2 result and a second random result (See Kocher Col. 6 Lines 47-49).

3 Regarding claims 2 and 20, Kocher disclosed calculating the output data item (OPN(D))
4 by performing an exclusive OR operation between the first and second random results (See
5 Kocher Col. 6 Lines 28-34 and 64-67).

6 Regarding claim 3, Kocher disclosed that the steps are performed during operations
7 relating to data calculated from the input message (See Kocher Col. 6 Paragraph 5).

8 Regarding claim 4, Kocher disclosed that a new random value is drawn at each new
9 execution of said operation of sequence of operations (See Kocher Fig. 1 Element 100).

10 Regarding claims 5-7, Kocher disclosed that steps are performed as part of an operation
11 or a sequence of operations performed On said secret key (See Kocher Col. 6 Paragraph 5),
12 wherein the cryptography algorithm is carried out in several calculation rounds comprising a
13 sequence of operations on the secret key K in order to supply, at each round, a corresponding
14 subkey (K_i), and wherein said steps are applied to said sequence of operations in order to supply,
15 at each round, a first random result (K_{iv}) and a second random result (K_{jz}) (See Kocher Col. 6
16 Paragraph 5 and Col. 10 Paragraph 3), and calculating an exclusive OR result between an input
17 data item for that round and the first random result (K_{iv}) in order to supply an intermediate
18 result and calculating an exclusive OR result between said intermediate result and the second
19 random result (K_{iz}) in order to supply an output data item for that round (See Kocher Col. 10
20 Line 61 – Col. 11 Line 5).

21 Claims 8, 14, 16, 18, and 23 are rejected for the same reasons as claim 4 above.

Regarding claim 10, Kocher disclosed that the cryptographic algorithm is the DES algorithm (See Kocher Abstract).

Claims 13, 15, and 17 are rejected for the same reasons as claim 3 above.

Regarding claims 21-22, Kocher disclosed that said cryptographic algorithm comprises a plurality of calculation rounds, and wherein said first and second random results are generated during each calculation round (See Kocher Col. 10 Line 39 – Col. 11 Line 26); and that said executing means performs the following steps during each calculation round: calculating an exclusive OR result between an input data item for that round and the first random result in order to supply an intermediate result and; calculating an exclusive OR result between said intermediate result and the second random result in order to supply an output data item for that round (See Kocher Col. 10 Line 61 – Col. 11 Line 5).

Conclusion

Claims 1-8, 10, and 13-23 have been rejected.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- a. Kocher et al. “Differential Power Analysis” disclosed how to perform DPA and various countermeasures to protect against DPA.

b. Schneier et al. "Twofish: A 128-Bit Block Cipher" disclosed that whitening an input to an encryption function increases the difficulty of key search attacks against an encryption system.

Art Unit: 2131

1 c. Chari et al. "Towards Sound Approaches to Counteract Power-Analysis Attacks"
2 disclosed a method which combined random data with input data prior to the first and last
3 four rounds of DES.

4 d. Kawamura et al. (US Patent Number 6,940,975) disclosed masking the input to a
5 round of DES with random data and then negating the masking at the beginning of the
6 next round.

7 e. Johnson et al. (US Patent Number 5,870,470) disclosed a system for masking a
8 keyblock which creates an intermediate part and then creates the masked key block.

9 f. Michel et al. (US Patent Number 5,625,690) disclosed a system which blinded the
10 input to a DES encryptor with random data and unblinded the data that was output of the
11 DES decryptor.


12 Any inquiry concerning this communication or earlier communications from the
13 examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790.
14 The examiner can normally be reached on M-F 8-4.

15 If attempts to reach the examiner by telephone are unsuccessful, the examiner's
16 supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the
17 organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Matthew Henning
Assistant Examiner
Art Unit 2131
11/21/2005



AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100